OA Cyber Security Plan FY 2019

Table of Contents

Vision 3

Goals, Strategies, and Tactics 5

Goal #1: Create a Culture that Fosters the Adoption of Cyber Security Best Practices 5

1.1 Strategy: Cyber Security Training 5

1.2 Strategy: Cyber Security Threat Awareness 6

1.3 Strategy: Emphasis on the Importance of Cyber Security by the Highest Level Executives 6

Goal #2: Use Cutting-Edge Technology to Protect State Assets 6

2.1 Strategy: Protect State Networks from Unauthorized Access and Denial of Service 6

2.2 Strategy: Protect State Data Centers and Data Center Infrastructure from Unauthorized Access 6

2.3 Strategy: Protect Computing Endpoints from Malicious Attack and Compromise 6

2.4 Strategy: Ensure Appropriate Access to Systems, Applications and Websites 7

2.5 Strategy: Protect Sensitive Data in Motion and at Rest from Unauthorized Access and Distribution 7

Goal #3: Respond to Cyber Security Incidents Swiftly and Effectively 7

3.1 Strategy: Prepare for Cyber Security Incidents through Planning and Exercises 7

3.2 Strategy: Assess the Current Cyber Security Threat Landscape through Internal and External Sources 7

Goal #4: Establish and Maintain IT Governance that Promotes Cyber Security 8

4.1 Strategy: Maintain Cyber Security Policies, Standards & Best Practices 8

4.2 Strategy: Perform Cyber Security Audits 8

4.3 Strategy: Data Governance 8

4.4 Strategy: Vendor Security Risk Management 8

Vision

The State of Missouri's vision for cyber security has state agencies doing the majority of their business electronically under conditions of acceptable risk to state assets. There are 3 major drivers for this vision:

- Citizens expect government to provide online services
- E-Government is seen as the lever to make government more effective and efficient
- Tomorrow's workforce relies on technology to do their job

While it is true that it would be much more difficult for identity thieves and hackers to obtain access to citizen data if systems, networks and databases didn't exist or were unplugged, that is not an acceptable situation. State agencies must use technology to effectively, efficiently and securely deliver services to citizens in the manner they expect – electronically. Citizens expect businesses and governments to provide services electronically so that they may access those services when, where and how they desire. Citizens want to interact with government through websites, social media, mobile applications and text messaging. The days of standing in line for service and/or mailing paper forms to a government agency are fading away.

Technology is often viewed as the lever that helps government deliver improved services more effectively and efficiently. Modern systems that capture and move data electronically are able to dramatically increase employee productivity through the use of document management, case management, workflow, messaging, etc. Implementation of these systems increases productivity, reduces processing/wait times, reduces postage/paper/print costs, reduces storage costs, reduces errors and increases customer and employee satisfaction levels. Systems like these have the ability to transform government and allow agencies to better manage limited resources.

In addition, the workforce is changing. Today's young people entering the workforce expect to use technologies like social media, unified communications and collaboration platforms to "get things done" across organizational boundaries. They expect to use mobile devices to work anywhere at any time and many expect to be able to use their own devices when doing so.

The State of Missouri's vision for cyber security must enable the above-described use of technology by citizens, state agencies and state employees while mitigating the risk to state assets. This is no small task and requires a comprehensive well-executed plan that meets the following four strategic goals:

- **Create a Culture that Fosters the Adoption of Cyber Security Best Practices**: All Missouri State employees must understand the importance of safeguarding state data and the importance of cyber security best practices – especially as they relate to their job. Informed and motivated state employees will ensure that those best practices are adhered to and made a routine part of conducting state business in Missouri. This includes the information technology (IT) professionals that work for the Information Technology Services Division (ITSD) of the Office of Administration (OA) and all other state employees working in fields other than IT.
- **Use Cutting-Edge Technology to Protect State Assets**: The State of Missouri's Chief Information Security Officer (CISO) and his/her team in the Office of Cyber Security (OCS), must be provided the latest tools in cyber security defense that can be utilized to protect the state's networks, systems, data and endpoints from malicious attacks.
- **Respond to Cyber Security Incidents Swiftly and Effectively**: The response to any State of Missouri cyber security incident must be swift and effective in order to mitigate the effect of any such incident. In order to

accomplish this, the CISO must establish the relationships with other entities, the plans for response and the systems for cyber security event management before an incident occurs.

- **Establish and Maintain IT Governance that Promotes Cyber Security**: The CIO and CISO must establish standards, policies and governance around all aspects of information technology that promote cyber security. Cyber security should be baked-in to contracts, projects and daily operations.

This cyber security plan outlines the strategies and tactics that will be employed by the State of Missouri to keep the state's networks, systems and data safe from identity thieves, hacktivists and international nation-state operatives. The plan uses a layered approach that brings technology and best practices together - enabling state employees to conduct business securely with a minimum amount of inconvenience, while mitigating risk to state networks, systems and data.

Goals, Strategies, and Tactics

Goal #1: Create a Culture that Fosters the Adoption of Cyber Security Best Practices

Cyber security is not achieved by a small number of highly trained IT professionals that sit in a room monitoring networks and defending the state against attackers. Those highly trained pros are vital to the task, but all state employees must participate if we are to solve the problem of protecting the state's networks, systems, data and other electronic assets.

State employees protect citizen information when they follow best practices while surfing the web, reading email, logging into an internal system, accessing citizen data or traveling with a mobile device. All state employees must take time to understand the best practices so that they can be a part of the solution and not part of the problem. Only then will we realize our goal of having all state employees working productively while adopting the best practices that help keep the state safe from cyber attacks.

To ensure that state employees are educated and are "cyber aware," the following strategies shall be pursued:

Cyber Security Training: State employees shall be trained and re-trained on cyber security best practices as they relate to their job.

Cyber Security Threat Awareness: State employees shall receive information about current cyber threats and the ways to combat those threats as that information becomes available.

Emphasis on the Importance of Cyber Security by the Highest Level Executives: There must be an emphasis on cyber security by state executives at the highest level including: Elected Officials, Department Directors, Division Directors and Commissioners.

1.1 Strategy: Cyber Security Training

Cyber security is everyone's responsibility and cyber security awareness and employee best practices are critical to the success of any plan. In fact, many cyber security threats are non-technical in nature and require employee awareness and good judgment to combat them. Education and training around cyber security and adherence to best practices is the best defense against these threats.

For example, consider a social engineering scam combined with spear phishing – in this case a hacker tricks a targeted victim into performing an action based on publicly available information about the victim. In this scam the attacker may use information that is publicly available on social media and organization websites to learn about the victim's job title, duties, co-worker names, friends, hobbies, etc. in order to craft an email that seems legitimate to the victim. This lures the victim to open an attachment or click a link in an email – often while using a device at work. Once that occurs, zero-day malware (malware unknown to Anti-Virus software) is downloaded onto the victim's machine and trouble ensues. The best way to stop these attacks is to educate employees about these types of attacks and prevent the malicious links from ever being clicked.

ITSD, together with the Center for Management & Professional Development and other state agencies, must educate state employees about how to safeguard citizen information and state assets from the attacks of cyber criminals. State employees must be trained regularly in best practices related to cyber security and the use of the Internet.

1.2 Strategy: Cyber Security Threat Awareness

1.3 Strategy: Emphasis on the Importance of Cyber Security by the Highest Level Executives

It is not realistic to expect an average state employee to recognize the importance of adopting good cyber security practices unless state executives at the highest levels do so first. Without determined leadership, cyber security will continue to be perceived as a burden that is unnecessarily placed on state employees by IT staff that don't understand "what needs to get done." However, if elected officials, department directors, division directors, commissioners and like leaders emphasize that cyber security is a foundational prerequisite of doing business electronically, then our culture can be changed to increase adherence to cyber security best practice.

Goal #2: Use Cutting-Edge Technology to Protect State Assets

It is imperative that the State of Missouri's cyber security professionals and state employees be given the technical tools they need to help them prevent successful cyber attacks. To this end, a budget has been dedicated towards new and existing cyber security initiatives.

ITSD's Office of Cyber Security (OCS) has identified the following five strategies to secure state networks, systems, data and assets through the use of technology:

- **Protect State Networks from Unauthorized Access and Denial of Service**
- **Protect State Data Centers and Data Center Infrastructure from Unauthorized Access**
- **Protect Computing Endpoints from Malicious Attack and Compromise**
- **Ensure Appropriate Access to Systems, Applications and Websites**
- **Protect Data in Motion and at Rest from Unauthorized Access and Distribution**

2.1 Strategy: Protect State Networks from Unauthorized Access and Denial of Service

There was a time when the cornerstone of cyber security strategy was limiting network access to authorized users and preventing access to anyone else. That strategy, which employs firewalls and intrusion prevention systems, is akin to building a moat around a castle and limiting entry to a drawbridge. While no longer the focal point of cyber security, this strategy still has a place in today's world.

2.2 Strategy: Protect State Data Centers and Data Center Infrastructure from Unauthorized Access

The physical security of the State Data Center (SDC), the state's secondary site, the state's server rooms and the infrastructure contained within those facilities is of the utmost importance. Technology plays an important role in ensuring that security.

2.3 Strategy: Protect Computing Endpoints from Malicious Attack and Compromise

In today's world protecting state networks and data centers from unauthorized intrusion is only the beginning of an effective security plan. That is because at any given time state employees are using their state issued computing devices to access information available outside the state network. They do this when visiting a website or opening an email. Each time a state employee interacts with the outside world in this manner, the possibility exists that they will be exposed to the malicious attack of a cyber-criminal, identity thief, hacktivist or state-sponsored cyber warrior. The state employs a variety of tactics that utilize technology to mitigate the risk that such actions will result in a security incident.

2.4 Strategy: Ensure Appropriate Access to Systems, Applications and Websites

The processes and systems involved in the identification of a user with their appropriate permissions comprise authentication and authorization management. Whenever users log onto workstations or applications, the users authenticate themselves using credentials and an authorization service describes what permissions to enable based on that user's group/role. Authentication and authorization can be accomplished at the application level so that users receive credentials for a specific application or at the enterprise level with single sign-on for all applications and data stores associated with the enterprise. In practice, the state uses a blend of those methods with a goal of moving away from one-off credentialing to the enterprise single sign-on method.

2.5 Strategy: Protect Sensitive Data in Motion and at Rest from Unauthorized Access and Distribution

The State of Missouri has petabytes (PB) of data in its possession. Some of that data is open data - available to the public on websites or via Missouri Sunshine Law requests. However, much of the data is sensitive and includes Personally Identifiable Information (PII) and can include Protected Health Information (PHI), credit card numbers, social security numbers and more. It is incumbent upon the State of Missouri and state employees to safeguard the privacy of citizen data whether it is at rest or in motion.

Goal #3: Respond to Cyber Security Incidents Swiftly and Effectively

Governments experience an ever-increasing number of cyber-attacks each day. Cyber-attackers are more determined than ever and are often very sophisticated in their methods, using social engineering and zero-day malware to infiltrate private networks and gain access to data. Thus, it is not a matter of IF the State will experience a cyber security incident, but a matter of WHEN the state will experience a cyber security incident. The strategies and tactics in this plan speak to limiting the number of successful attacks and minimizing the damage such attacks will cause. While the technologies and training discussed previously are critical to reducing the number of successful attacks, the quality of incident response plays a major role in minimizing the scope and damage of incidents. ITSD's Office of Cyber Security (OCS) has identified the following strategies to respond to cyber security incidents swiftly and effectively:

- **Prepare for Cyber Security Incidents through Planning and Exercises**
- **Assess the Current Cyber Security Threat Landscape through Internal and External Sources**

3.1 Strategy: Prepare for Cyber Security Incidents through Planning and Exercises

Just like sports teams practice internally before facing their next rival, ITSD and state agencies must work together to ensure that essential state functions maintain operational status during and after a cyber security event. By planning for and simulating some of the worst known attacks, ITSD can recover essential assets quicker and provide agencies insight to the continuity of their operations.

3.2 Strategy: Assess the Current Cyber Security Threat Landscape through Internal and External Sources

Understanding the current cyber security threat landscape enables ITSD to quickly react to vulnerabilities and other exploits before they impact state government functions. By understanding critical system and network events in near real time, ITSD can identify and fix security concerns and in the event of an attack, gather information about the incident and begin the remediation steps. ITSD also looks outward, analyzing cyber security information coming from vendors and various state and federal agencies.

Goal #4: Establish and Maintain IT Governance that Promotes Cyber Security

IT governance results in processes that ensure that IT organizations function as intended. It is important that ITSD use IT governance to ensure that cyber security is "baked into" the way state employees use and develop technology every day. With respect to cyber security, IT governance includes the policies, processes, and audits that together establish controls around the way IT systems are used and state data is handled. To establish and maintain IT governance that promotes cyber security, the following strategies shall be pursued:

- **Maintain Cyber Security Policies, Standards, & Best Practices**
- **Perform Cyber Security Audits**
- **Data Governance**

4.1 Strategy: Maintain Cyber Security Policies, Standards & Best Practices

ITSD creates security policies to protect data and to ensure the continuity of state government. These policies enable state employees to do their job within a framework that provides an appropriate level of security for state assets and data. Examples of policy include the “SafeBoot” policy (laptops must use disk encryption) and the Active Directory strong password policy (passwords must be of minimum length and contain complex characters).

ITSD also maintains enterprise security standards and provides guidance to all state agencies. These standards are typically drafted by individuals from multiple agencies and then approved by the Information Technology Advisory Board (ITAB). The standards utilized by ITSD are derived from the NIST security framework - the security framework that federal agencies follow to secure data and ensure business continuity. On a regular basis, OCS reviews the state security standards to ensure they are relevant and adhere to the latest guidance from NIST and other authoritative sources.

In addition, OCS provides guidance to ITSD's functional areas like application development, networks and the State Data Center so that best practices for their functions can be established.

4.2 Strategy: Perform Cyber Security Audits

Cyber security audits help determine if best practices are being followed by the IT administrators and developers. Information gleaned from those audits also forms the basis for developing a correction plan to resolve known issues.

4.3 Strategy: Data Governance

The term data governance refers to the policies and procedures around how data is stored, transported and accessed. These policies and procedures control the rights and responsibilities over data so that the integrity of data can be assured and data remains secure.

In state government, the majority of data belongs to state agencies that "own" the data and make decisions about its content, its use and the authorized access to it. ITSD is the technical custodian of data and is responsible for maintaining the systems that store, transport, and display data. This makes it imperative that state agencies and ITSD work closely together on data governance.

4.4 Strategy: Vendor Security Risk Management

While the State of Missouri has elevated its security posture over the last 5 years, one type of risk has remained elusive in monitoring and mitigating: vendor risk. While contracts establish security requirements and expectations with vendors, they do not shed visibility into the company’s real practices and overall cyber hygiene. Vendors have been the

initial attack vector to gain access to multiple targets that lead to massive breaches. Home Depot (56m credit card numbers), Target (40m credit card numbers), and closer to home a healthcare organization in Farmington, MO (48,000 SSNs incl. healthcare info) are just a few entities impacted by security lapses within their vendor partnerships. Understanding and mitigating vendor security risk is vital in safeguarding sensitive information.